УТВЕРЖДЕНЫ
приказом АО «Мидзухо Банк (Москва)»
от 27.08.2025 № 71/25

Президент А.И. Малышев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 40601D00C99450EB8BEAF69867AF066C
Владелец: МАЛЫШЕВ АЛЕКСАНДР ИЛЬИЧ
Действителен: с 14.02.2025 до 14.12.2037

Базовые рекомендации

по защите информации при работе в ДБО

и возможные риски получения несанкционированного доступа к защищаемой информации

Москва

Август 2025 / Редакция №1

Настоящие Базовые рекомендации по защите информации от воздействия программных кодов (вредоносного кода), приводящих к нарушению штатного функционирования средств вычислительной техники, в целях противодействия осуществлению переводов денежных средств без согласия клиента, разработаны в соответствии с в Положением Банка России № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента целях ознакомления с возможными рисками и мерами по минимизации рисков несанкционированного доступа к защищаемой информации».

В ходе работы с системой дистанционного банковского обслуживания (ДБО) **возможны следующие риски** получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения денежными средствами:

- Заражение компьютера используемого для подключения к системе ДБО.

  Заражение обычно происходит путем посещения неблагонадежных веб-сайтов в сети «Интернет», на которых размещаются вредоносные вложения или настроена скрытая переадресация на вредоносные веб-сайты.

- Заражение устройства через съёмные носители информации.

  Заражение через съёмные носители информации (внешние жесткие диски, флэш-носители, CD или DVD-диски) может быть реализовано путем использования носителей с непроверенным содержимым и полученных от неизвестных. Это могут быть копии вредоносного ПО, замаскированные под различные приложения.

- Целевые фишинговые рассылки по электронной почте.

  Фишинговые рассылки содержат в себе «привлекательное» содержание и вложение для клиентов с целью перехода клиентов по ложным ссылкам и компрометации критичной информацией. При открытии такого вложенного файла или перехода по ссылке в письме на устройство загружается вредоносное программное обеспечение. Под фишинговыми рассылками также подразумевается отправка файлов и документов от партнеров и знакомых клиентов.

В результате реализации перечисленных рисков возможны:

- Утечка конфиденциальной информации, логинов/паролей.
- Выполнение на компьютере злонамеренных действий.
- Проникновение вирусов-шифровальщиков и иного ПО, которое может привести к неработоспособности компьютера.
- Непосредственно операции по выводу денег.

В целях противодействия осуществлению переводов денежных средств без согласия Клиента АО «Мидзухо Банк (Москва)» (далее по тексту – «Банк») рекомендует следующие меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого Клиентом осуществлялся перевод денежных средств необходимо внедрить следующие меры по предотвращению несанкционированного доступа к защищаемой информации:

- Не используйте компьютер с системой ДБО для посещения сайтов в сети Интернет. Используйте выделенный компьютер только для работы с ДБО.
- На выделенном для работы с ДБО компьютере установите антивирусное программное обеспечения для защиты от вредоносного ПО.
- Не подключайте компьютер, используемый для работы с ДБО, к общественным Wi-Fi сетям.
- Не открывайте письма, полученные из неизвестных источников на компьютере, используемых для работы с ДБО, не открывайте вложенные файлы и не переходите по ссылкам на веб-сайты.
- Не подключайте к компьютеру, используемому для работы с ДБО флэш-носители, CD или DVD-диски с непроверенным содержимым.
- Не устанавливайте и не открывайте вложения от Банка по нетипичным каналам связи.
- Используйте информацию с официального сайта Банка для установки и настройки системы ДБО. Не используйте переход к указанным сервисам и установку клиентской части системы ДБО по ссылке из других источников.
- В операционной системе работайте под учетной записью обычного пользователя (не администратор). Защитите вход в операционную систему надежным сложным паролем.
- Блокируйте компьютер при временном отсутствии на рабочем месте, а при длительном отсутствии обязательно выключайте компьютер. Настройте автоматическую блокировку компьютера по истечении определённого времени (не более 5 минут).
- Не оставляйте без контроля ключевой носитель, используемый для работы с системой ДБО. Извлекайте ключевой носитель после завершения работы с системой ДБО. Храните носитель отдельно от компьютера в местах, исключающих несанкционированный доступ к носителю.

Каналы коммуникации с Банком

- Используйте для коммуникаций с АО «Мидзухо Банк (Москва)» только официальные каналы коммуникации.
- Система ДБО является защищенным каналом связи, поэтому она более предпочтительна для обмена электронными копиями документов.
- Если у Вас (у Клиента) возникли сомнения в том, что к Вам обращается именно представитель Банка, рекомендуем обратиться в Банк по официальным каналам и получить подтверждение.

- Представитель Банка никогда не будет запрашивать у Вас какую-то конфиденциальную информацию, связанную с Вами, либо с Вашим счетом. Тем более не будет предлагать совершить какие-то срочные действия.

Если вы обнаружили:

- операции, которые не совершали: смена пароля, создание платежей;
- видите на компьютере действия, которых не совершаете: перемещение курсора, открытие и закрытие окон, заполнение полей документа;
- данные для входа стали известны посторонним

Незамедлительно свяжитесь со службой поддержки Банка по телефону 8-495-212-03-40.